

SHUB & JOHNS LLC

Jonathan Shub (No. 237708)
Benjamin F. Johns
Samantha E. Holbrook
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
jshub@shublawayers.com
bjohns@shublawayers.com
sholbrook@shublawayers.com

Attorneys for Plaintiff

**IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA**

MATTHEW RUTLEDGE, individually
and on behalf of all others similarly
situated,

Plaintiff,

v.

KEENAN PRODUCTION SOLUTIONS,
LLC,

Defendant.

Case No.:

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Matthew Rutledge (“Plaintiff” or “Rutledge”), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Keenan & Associates (“Keenan” or “Defendant”), based upon personal knowledge with respect to himself and upon information and belief derived from, among other things, investigation of counsel

1 and review of public documents as to all other matters:

2 **NATURE OF THE ACTION**

3
4 1. This class action arises out of the recent data breach (the “Data
5 Breach”) involving Keenan, which collected and stored certain personally
6 identifiable information (“PII”) and protected health information (“PHI”) (collectively,
7 “Private Information”) of the Plaintiff and the putative Class Members.
8

9 2. According to Keenan, the PII and PHI compromised in the Data
10 Breach included highly-sensitive information including dates of birth, Social
11 Security numbers, passport numbers, driver’s license numbers, health insurance
12 information, and other general health information.¹
13

14 3. Social Security numbers are particularly valuable to criminals. This
15 information can be sold and traded on the dark web black market. The compromise
16 of a Social Security number is particularly troubling because it cannot be easily
17 changed and can be misused in a range of nefarious activities, such as filing
18 fraudulent tax returns to steal tax refund payments, opening new accounts to take
19 out loans, and other forms of identity theft.
20
21

22 4. The Data Breach was a direct result of Keenan’s failure to implement
23 adequate and reasonable cybersecurity procedures and protocols necessary to
24
25

26
27 ¹ Sample Keenan *Notice of Data Security Incident*, available at
28 https://oag.ca.gov/system/files/EXPERIAN_K7150_KeenanAssociates_Notice%20Letter_Redacted.pdf (last accessed Feb. 2, 2024) (hereinafter, “Notice”).

1 protect consumers' Private Information. Keenan has acknowledged that the
2 cybersecurity attack occurred "at various times between August 21, 2023 and
3 August 27, 2023," but that it waited until January 26, 2024 to begin contacting
4 Class Members. *Id.*

6 5. According to a notice of data breach filed with the Attorney General of
7 Maine, the Data Breach has affected 1,509,616 individuals.²

9 6. This was not a passive data breach where, for example, it is unclear
10 whether the compromised data was targeted or even seen. By Keenan's own
11 acknowledgement, the data breach here occurred because an "unauthorized third
12 party" was able to "gain[] access to" and "obtain[]" data from Keenan's internal
13 computer systems.³

15 7. Plaintiff brings this lawsuit on behalf of himself and all of those
16 similarly situated to address Keenan's inadequate safeguarding of Class Members'
17 Private Information that it collected and maintained, and for failing to provide
18 timely and adequate notice to Plaintiff and other Class Members that their
19 information was unsecured and left open to the unauthorized access of any
20 unknown third party.
21
22
23
24
25

26 ² [https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-](https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml)
27 [a3be3e84a7d0.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml) (last accessed Feb. 2, 2024).

28 ³ *Id.*

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) the amount in controversy exceeds \$5 million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiff Rutledge has different citizenship from Defendant. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiffs and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

PARTIES

Plaintiffs

10. Plaintiff Matthew Rutledge is an adult, who at all relevant times, was a resident and citizen of San Bernardino County in the state of California.

11. Based on his comprehensive and recent relationship with Keenan, Plaintiff Rutledge has a good faith belief that his Private Information was compromised in the Data Breach that occurred on or around August 21, 2023.

12. Beginning right around the time the Data Breach occurred in August

1 2023, Plaintiff Rutledge began to receive notifications that someone had made login
2 attempts and attempted to change his passwords for his existing accounts with credit
3 reporting agencies, online survey websites, and his personal email account. He also
4 received notifications from companies who pulled his credit report despite the fact
5 that he never made any requests or engaged in transactions that would merit pulling
6 his credit report.
7
8

9 13. Plaintiff Rutledge has spent several hours addressing the unauthorized
10 activity and otherwise monitoring his accounts as a result of the Data Breach. The
11 time spent dealing with these incidents resulting from the Data Breach is time
12 Plaintiff Rutledge otherwise would have spent on other activities, such as work
13 and/or recreation.
14
15

16 14. Plaintiff Rutledge plans on taking additional time-consuming,
17 necessary steps to help mitigate the harm caused by the Data Breach, including
18 continually reviewing his accounts for any unauthorized activity.
19

20 **Defendant**

21 15. Defendant Keenan & Associates is an insurance consulting and
22 brokerage firm who services schools, public agencies, and health care
23 organizations.⁴ Its principal place of business and headquarters is located at 2355
24
25
26

27 ⁴ See *About Keenan*, KEENAN <https://www.keenan.com/About> (last visited Feb. 2,
28 2024).

1 Crenshaw Blvd., Suite 200, Torrance, California 90501.⁵

2 **FACTUAL ALLEGATIONS**

3
4 16. Keenan sells employee benefits, workers compensation coverage, and
5 property & liability coverage to California educational institutions, public agencies
6 and health care organizations.⁶

7
8 17. Due to the nature of the services Keenan provides, it receives and is
9 entrusted with securely storing consumers' Private Information, which includes,
10 *inter alia*, individuals' full name, date of birth, Social Security number, passport
11 number, driver's license number, health insurance information, and general health
12 information.
13

14 **Keenan's Unsecure Data Management and Disclosure of Data Breach**

15
16 18. Plaintiff and Class Members provided their Private Information to
17 Keenan with the reasonable expectation and mutual understanding that Keenan
18 would comply with its obligations to keep such information confidential and secure
19 from unauthorized access.
20

21 19. Data security is purportedly a critical component of Keenan's business
22 model. On a section of its website entitled "Privacy Policy," Keenan makes the
23

24
25
26 ⁵ [https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-](https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml)
27 [a3be3e84a7d0.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml) (last accessed Feb. 2, 2024).

28 ⁶ <https://www.keenan.com/Solutions> (last visited Feb. 2, 2024).

1 following statements:⁷

- 2 • Keenan & Associates (including our affiliates and subsidiaries)
- 3 (“Keenan”, “we”, “us” or “our”) respects your privacy and takes our
- 4 privacy responsibility very seriously and **is committed to protecting it in**
- 5 **a manner consistent with applicable law** and this statement.
- 6 • This Policy and notice applies to your Personal Information that we may
- 7 collect, use, receive, and disclose and describes our practices for
- 8 collecting, using, maintaining, protecting and disclosing that information
- 9 in the course of providing our services.
- 10 • **We have implemented measures reasonably designed to protect and**
- 11 **secure your Personal Information from** accidental loss, misuse, and
- 12 **from unauthorized access, use, alteration, and disclosure.**

13 20. Keenan also maintains a “California Privacy Policy”, which contains

14 information concerning the requirements of California Consumer Privacy Act

15 (“CCPA”) as it relates to the storage of the data of California residents.⁸ A section

16 of the California Privacy Policy, under the header “Why We Collect Personal

17 Information and How We Use It,” delineates the various circumstances under which

18 Keenan may share PII and PHI for legitimate business purposes. It does not include

19 providing that data to “unauthorized third parties”; to the contrary, the Policy states

20 that “[w]e may disclose your personal information to a third party for a business or

21 that “[w]e may disclose your personal information to a third party for a business or

22 that “[w]e may disclose your personal information to a third party for a business or

23

24

25

26 ⁷ <https://www.keenan.com/Privacy-Statement> (last visited Feb. 2, 2024) (all emphasis

27 supplied).

28 ⁸ <https://www.keenan.com/CCPA> (last visited Feb. 2, 2024).

1 legal purpose” and “[w]e do not sell your personal information to third parties.”⁹

2 21. Contrary were Keenan’s various express assurances that it would take
3 reasonable measures to safeguard the sensitive information entrusted to it – and
4 only share it for an express authorized persons – an “unauthorized” person or
5 persons was able to access its network servers.
6

7 22. According to its January 26, 2024 Notice letter concerning the breach,
8 on August 27, 2023, Keenan “noticed disruptions occurring on some Keenan
9 network servers” and “immediately began an investigation and engaged leading
10 third-party cyber security and forensic experts to assist.” It later determined that a
11 “an unauthorized party gained access to certain Keenan internal systems at various
12 times between approximately August 21, 2023 and August 27, 2023, and that the
13 unauthorized party obtained some data from Keenan systems.”
14
15
16

17 23. The database files that were compromised included names, mailing
18 addresses, Social Security numbers, personal health information, and other
19 information related to prior productions.
20

21 24. To date, Keenan has not disclosed specifics of the attack, such as
22 whether ransomware has been used. It has only told the Maine AG’s Office that the
23 breach was an “[e]xternal system breach (hacking).”
24

25 25. As such, Keenan failed to secure the PII and PHI of the individuals that
26

27 _____
28 ⁹ *Id.*

1 provided it with this sensitive information. It failed to take appropriate steps to
2 protect the PII and PHI of Plaintiff and other Class Members from being disclosed.

3
4 **Keenan is a HIPAA Covered Entity**

5 26. As a regular and necessary part of its business, Keenan collects and
6 custodies the highly sensitive Private Information of its clients' employees. Indeed,
7 the Data Breach notice states that "health insurance information" and "general
8 health information" were among the types of information compromised in the
9 breach. Keenan is, therefore, required under federal and state law to maintain the
10 strictest confidentiality of the patient's Private Information that it requires, receives,
11 and collects, and Keenan is further required to maintain sufficient safeguards to
12 protect that Private Information from being accessed by unauthorized third parties.
13
14

15 27. Indeed, Keenan's Privacy Policy acknowledges that "[s]ome of the
16 categories of Personal Information that we may collect are special categories of
17 information protected by federal law including your health records (such as your
18 medical history and reports on medical diagnoses, injuries, and treatment)...".¹⁰
19
20

21 28. As a HIPAA covered entity, Keenan is required to ensure that it will
22 implement adequate safeguards to prevent unauthorized use or disclosure of Private
23 Information, including by implementing requirements of the HIPAA Security Rule
24 and to report any unauthorized use or disclosure of Private Information, including
25
26

27
28 ¹⁰ See <https://www.keenan.com/Privacy-Statement> (last accessed Feb. 2, 2024).

1 incidents that constitute breaches of unsecured protected health information as in
2 the case of the Data Breach complained of herein.

3
4 29. Due to the nature of Keenan's business, which includes providing
5 group health insurance to employers, Keenan would be unable to engage in its
6 regular business activities without collecting and aggregating Private Information
7 that it knows and understands to be sensitive and confidential.
8

9 30. Plaintiffs and the Class Members relied on Keenan to implement and
10 follow adequate data security policies and protocols, to keep their Private
11 Information confidential and securely maintained, to use such Private Information
12 solely for business and health care purposes, and to prevent the unauthorized
13 disclosures of the Private Information. Plaintiffs and Class Members reasonably
14 expected that Keenan would safeguard their highly sensitive information and keep
15 their Private Information confidential.
16
17

18 31. As described throughout this Complaint, Keenan did not reasonably
19 protect, secure, or store Plaintiffs' and the Class's Sensitive Information prior to,
20 during, or after the Data Breach, but rather, enacted unreasonable data security
21 measures that it knew or should have known were insufficient to reasonably protect
22 the highly sensitive information Keenan maintained. Consequently, Keenan allowed
23 for the exfiltration of Plaintiff and Class Members' Private Information.
24
25
26
27
28

1 **Keenan Failed to Comply with FTC Guidelines**

2 32. Keenan was prohibited by the Federal Trade Commission Act (the
3 “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices
4 in or affecting commerce.” The Federal Trade Commission (the “FTC”) has
5 concluded that a company’s failure to maintain reasonable and appropriate data
6 security for consumers’ sensitive personal information is an “unfair practice” in
7 violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d
8 236 (3d Cir. 2015).

9 33. The FTC has promulgated numerous guides for businesses which
10 highlight the importance of implementing reasonable data security practices.
11 According to the FTC, the need for data security should be factored into all business
12 decision-making.

13 34. In 2016, the FTC updated its publication, *Protecting Personal*
14 *Information: A Guide for Business*, which established cyber-security guidelines for
15 businesses. The guidelines note that businesses should protect the personal
16 customer information that they keep; properly dispose of personal information that
17 is no longer needed; encrypt information stored on computer networks; understand
18 their network’s vulnerabilities; and implement policies to correct any security
19 problems.¹¹ The guidelines also recommend that businesses use an intrusion
20

21
22
23
24
25
26
27
28 ¹¹ *See* <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last accessed Feb. 2, 2024).

1 detection system to expose a breach as soon as it occurs; monitor all incoming
2 traffic for activity indicating someone is attempting to hack the system; watch for
3 large amounts of data being transmitted from the system; and have a response plan
4 ready in the event of a breach. *Id.*

6 35. The FTC further recommends that companies not maintain PII longer
7 than is needed for authorization of a transaction; limit access to sensitive data;
8 require complex passwords to be used on networks; use industry-tested methods for
9 security; monitor for suspicious activity on the network; and verify that third-party
10 service providers have implemented reasonable security measures.

13 36. The FTC has brought enforcement actions against businesses for
14 failing to adequately and reasonably protect customer data, treating the failure to
15 employ reasonable and appropriate measures to protect against unauthorized access
16 to confidential consumer data as an unfair act or practice prohibited by Section 5 of
17 the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting
18 from these actions further clarify the measures businesses must take to meet their
19 data security obligations.

22 37. These FTC enforcement actions include actions against healthcare
23 providers and partners like Keenan. *See, e.g., In the Matter of Labmd, Inc., A Corp.*,
24 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28,
25 2016) (“[T]he Commission concludes that LabMD’s data security practices were
26
27
28

1 unreasonable and constitute an unfair act or practice in violation of Section 5 of the
2 FTC Act.”)

3
4 38. Keenan failed to properly implement basic data security practices.

5 39. Keenan’s failure to employ reasonable and appropriate measures to
6 protect against unauthorized access to customers’ Private Information constitutes an
7 unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.
8

9 40. Keenan was at all times fully aware of the obligation to protect the
10 Private Information of customers and patients. Keenan was also aware of the
11 significant repercussions that would result from its failure to do so.
12

13 **Keenan Violated its HIPAA Obligations to Safeguard the Private**
14 **Information**

15 41. Keenan is a covered entity under HIPAA as a business associate (45
16 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and
17 Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for
18 Privacy of Individually Identifiable Health Information”), and Security Rule
19 (“Security Standards for the Protection of Electronic Protected Health
20 Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.
21
22
23
24
25
26
27
28

1 42. Keenan is subject to the rules and regulations for safeguarding
2 electronic forms of medical information pursuant to the Health Information
3 Technology Act (“HITECH”).¹² See 42 U.S.C. §17921, 45 C.F.R. § 160.103.
4

5 43. HIPAA’s Privacy Rule or *Standards for Privacy of Individually*
6 *Identifiable Health Information* establishes national standards for the protection of
7 health information that is kept or transferred in electronic form.
8

9 44. HIPAA requires “compl[iance] with the applicable standards,
10 implementation specifications, and requirements” of HIPAA “with respect to
11 electronic protected health information.” 45 C.F.R. § 164.302.
12

13 45. “Electronic protected health information” is “individually identifiable
14 health information ... that is (i) transmitted by electronic media; maintained in
15 electronic media.” 45 C.F.R. § 160.103.
16

17 a. HIPAA’s Security Rule requires Keenan to do the following:

18 b. Ensure the confidentiality, integrity, and availability of all electronic
19 protected health information the covered entity or business associate
20 creates, receives, maintains, or transmits;
21

22 c. Protect against any reasonably anticipated threats or hazards to the
23 security or integrity of such information;
24
25
26

27 ¹² See [https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-](https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/)
28 [health-medical-records/](https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/) (last accessed Feb. 2, 2024).

1 d. Protect against any reasonably anticipated uses or disclosures of such
2 information that are not permitted; and

3 e. Ensure compliance by its workforce.
4

5 46. HIPAA also requires Keenan to “review and modify the security
6 measures implemented . . . as needed to continue provision of reasonable and
7 appropriate protection of electronic protected health information.” 45 C.F.R. §
8 164.306(e). Additionally, Keenan is required under HIPAA to “[i]mplement
9 technical policies and procedures for electronic information systems that maintain
10 electronic protected health information to allow access only to those persons or
11 software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).
12
13

14 47. HIPAA and HITECH also obligated Keenan to implement policies and
15 procedures to prevent, detect, contain, and correct security violations, and to protect
16 against uses or disclosures of electronic protected health information that are
17 reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. §
18 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.
19
20

21 48. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also
22 requires Keenan to provide notice of the Data Breach to each affected individual
23 “without unreasonable delay and in no case later than 60 days following discovery
24
25
26
27
28

1 of the breach.”¹³

2 49. HIPAA requires a covered entity to have and apply appropriate
3 sanctions against members of its workforce who fail to comply with the privacy
4 policies and procedures of the covered entity or the requirements of 45 C.F.R. Part
5 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).
6

7 50. HIPAA requires a covered entity to mitigate, to the extent practicable,
8 any harmful effect that is known to the covered entity of a use or disclosure of
9 protected health information in violation of its policies and procedures or the
10 requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business
11 associate. *See* 45 C.F.R. § 164.530(f).
12

13 51. HIPAA also requires the Office of Civil Rights (“OCR”), within the
14 Department of Health and Human Services (“HHS”), to issue annual guidance
15 documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§
16 164.302-164.318. For example, “HHS has developed guidance and tools to assist
17 HIPAA covered entities in identifying and implementing the most cost effective and
18 appropriate administrative, physical, and technical safeguards to protect the
19 confidentiality, integrity, and availability of e-PHI and comply with the risk
20 analysis requirements of the Security Rule.” US Department of Health & Human
21
22
23
24

25
26
27 ¹³ *See* Breach Notification Rule, U.S. Dep’t of Health & Human Services,
28 <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (last
accessed Feb. 2, 2024).

Services, Security Rule Guidance Material.¹⁴ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.¹⁵

52. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PII like the data Keenan left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

53. A Data Breach such as the one Keenan experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which

¹⁴ See <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last accessed Feb. 2, 2024).

¹⁵ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last accessed Feb. 2, 2024).

1 compromises the security or privacy of the PHI.” *See* 45
2 C.F.R. 164.40

3 54. The Data Breach resulted from a combination of insufficiencies that
4 demonstrate Keenan failed to comply with safeguards mandated by HIPAA
5 regulations.
6

7 **Plaintiff and the Class Have Suffered Injury as a Result of Keenan’s**
8 **Data Mismanagement**

9 55. As a result of Keenan’s failure to implement and follow even the most
10 basic security procedures, Plaintiff’s and Class Members’ PII and PHI has been and
11 is now in the hands of an unauthorized third-party which may include thieves,
12 unknown criminals, banks, credit companies, and other potentially hostile
13 individuals. Plaintiff and other Class Members now face an increased risk of
14 identity theft, particularly due to the dissemination of their Social Security Number,
15 and will consequentially have to spend, and will continue to spend, significant time
16 and money to protect themselves due to Keenan’s Data Breach.
17
18

19 56. Plaintiff and other Class Members have had their most personal and
20 sensitive Private Information disseminated to the public at large and have
21 experienced and will continue to experience emotional pain and mental anguish and
22 embarrassment.
23
24

25 57. Plaintiff and Class Members face an increased risk of identity theft,
26 phishing attacks, and related cybercrimes because of the Data Breach. Those
27
28

1 impacted are under heightened and prolonged anxiety and fear, as they will be at
2 risk for falling victim for cybercrimes for years to come.

3
4 58. PII is a valuable property right.¹⁶ The value of PII as a commodity is
5 measurable. “Firms are now able to attain significant market valuations by
6 employing business models predicated on the successful use of personal data within
7 the existing legal and regulatory frameworks.”¹⁷ American companies are estimated
8 to have spent over \$19 billion on acquiring personal data of consumers in 2018.¹⁸ It
9 is so valuable to identity thieves that once PII has been disclosed, criminals often
10 trade it on the “cyber black-market,” or the “dark web,” for many years.
11
12

13 59. As a result of its real value and the recent large-scale data breaches,
14 identity thieves and cyber criminals have openly posted credit card numbers, Social
15 Security numbers, PII, and other sensitive information directly on various Internet
16 websites, making the information publicly available. This information from various
17
18

19 ¹⁶ See Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN
20 INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015),
21 [https://www.researchgate.net/publication/283668023_](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data)
22 [The_Value_of_Personal_Data](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data) (“The value of [personal] information is well
23 understood by marketers who try to collect as much data about personal conducts and
24 preferences as possible...”).

24 ¹⁷ *Exploring the Economics of Personal Data: A Survey of Methodologies for*
25 *Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), [https://www.oecd-](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)
26 [ilibrary.org/science-and-technology/exploring-the-economics-of-personal-](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)
27 [data_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en).

27 ¹⁸ U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-
28 Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU
(Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

1 breaches, including the information exposed in the Data Breach, can be aggregated
2 and become more valuable to thieves and more damaging to victims.

3
4 60. Personal information can be sold at a price ranging from \$40 to \$200,
5 and bank details have a price range of \$50 to \$200.¹⁹ Experian reports that a stolen
6 credit or debit card number can sell for \$5 to \$110 on the dark web.²⁰ Criminals can
7 also purchase access to entire company data breaches from \$900 to \$4,500.²¹
8

9 61. Consumers place a high value on the privacy of that data. Researchers
10 shed light on how much consumers value their data privacy—and the amount is
11 considerable. Indeed, studies confirm that “when privacy information is made more
12 salient and accessible, some consumers are willing to pay a premium to purchase
13 from privacy protective websites.”²²
14
15

16 62. Given these facts, any company that transacts business with a
17 consumer and then compromises the privacy of consumers’ PII has thus deprived
18

19 ¹⁹ Anita George, *Your personal data is for sale on the dark web. Here’s how much it*
20 *costs*, Digital Trends (Oct. 16, 2019),
21 <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

22 ²⁰ Brian Stack, *Here’s How Much Your Personal Information Is Selling for on the*
23 *Dark Web*, Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

24 ²¹ *In the Dark*, VPNOverview.com, 2019,
25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed on
26 Feb. 2, 2024).

27 ²² Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing*
28 *Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254
(June 2011), <https://www.jstor.org/stable/23015560?seq=1>.

1 that consumer of the full monetary value of the consumer's transaction with the
2 company.

3
4 63. Cyberattacks have become so notorious that the FBI and U.S. Secret
5 Service have issued a warning to potential targets so they are aware of, and
6 prepared for, a potential attack. As one report explained, "[e]ntities like smaller
7 municipalities and hospitals are attractive to ransomware criminals... because they
8 often have lesser IT defenses and a high incentive to regain access to their data
9 quickly.²³
10

11
12 64. Plaintiff and members of the Class, as a whole, must immediately
13 devote time, energy, and money to: 1) closely monitor their bills, records, and credit
14 and financial accounts; 2) change login and password information on any sensitive
15 account even more frequently than they already do; 3) more carefully screen and
16 scrutinize phone calls, emails, and other communications to ensure that they are not
17 being targeted in a social engineering or spear phishing attack; and 4) search for
18 suitable identity theft protection and credit monitoring services, and pay to procure
19 them.
20
21

22
23 65. Once PII is exposed, there is virtually no way to ensure that the
24 exposed information has been fully recovered or contained against future misuse.
25

26
27 ²³ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov.
28 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Feb. 2, 2024).

1 For this reason, Plaintiff and Class Members will need to maintain these heightened
2 measures for years, and possibly their entire lives, as a result of Keenan's conduct.
3
4 Further, the value of Plaintiff's and Class Members' Private Information has been
5 diminished by its exposure in the Data Breach.

6 66. As a result of Keenan's failures, Plaintiff and Class Members are at
7
8 substantial risk of suffering identity theft and fraud or misuse of their Private
9 Information.

10 67. Plaintiff and members of the Class suffered actual injury from having
11
12 PII compromised as a result of Keenan's negligent data management and resulting
13 Data Breach including, but not limited to (a) damage to and diminution in the value
14 of their PII, a form of property that Keenan obtained from Plaintiff; (b) violation of
15 their privacy rights; and (c) present and increased risk arising from the identity theft
16 and fraud.

17
18 68. For the reasons mentioned above, Keenan's conduct, which allowed
19
20 the Data Breach to occur, caused Plaintiff and members of the Class these
21 significant injuries and harm.

22 69. Plaintiff brings this class action against Keenan for their failure to
23
24 properly secure and safeguard Private Information and for failing to provide timely,
25 accurate, and adequate notice to Plaintiff and other Class Members that their Private
26 Information had been compromised.
27
28

1 70. Plaintiff, individually and on behalf of all other similarly situated
2 individuals, alleges claims in negligence, negligence *per se*, breach of implied
3 contract, breach of fiduciary duty, unjust enrichment, violations of the California
4 Consumer Privacy Act and California Legal Remedies Act, and California's Unfair
5 Competition Law.
6

7
8 **CLASS ACTION ALLEGATIONS**

9 71. Plaintiff brings this action on behalf of himself and on behalf of all
10 other persons similarly situated ("the Class"):
11

12 **Nationwide Class**

13 All individuals residing in the United States whose Private
14 Information was compromised as a result of the Data Breach,
15 including all individuals who were sent the Notice of the Data
Breach on or around January 26, 2024.

16 In the alternative, Plaintiff seeks to represent the following California class
17 (together with the Nationwide Class, the "Class"):
18

19 **California Class**

20 All individuals residing in California whose Private Information
21 was compromised as a result of the Data Breach, including all
22 individuals in California who were sent the Notice of the Data
23 Breach on or around January 26, 2024.

24 72. Excluded from the Class are Keenan's officers and directors, and any
25 entity in which Keenan has a controlling interest; and the affiliates, legal
26 representatives, attorneys, successors, heirs, and assigns of Keenan. Excluded also
27 from the Class are members of the judiciary to whom this case is assigned, their
28

1 families and members of their staff.

2 73. **Numerosity:** The members of the Class are so numerous that joinder
3 of all of them is impracticable. As noted above, there are approximately 1,509,616
4 consumers affected.
5

6 74. **Existence/Predominance of Common Questions of Fact and Law:**
7
8 There are questions of law and fact common to the Class, which predominate over
9 any questions affecting only individual Class Members. These common questions of
10 law and fact include, without limitation:
11

- 12 a. Whether Keenan unlawfully used, maintained, lost, or disclosed
13 Plaintiff's and Class Members' PII and PHI;
- 14 b. Whether Keenan failed to implement and maintain reasonable security
15 procedures and practices appropriate to the nature and scope of the
16 information compromised in the Data Breach;
- 17 c. Whether Keenan's data security systems prior to and during the Data
18 Breach complied with applicable data security laws and regulations;
- 19 d. Whether Keenan's data security systems prior to and during the Data
20 Breach were consistent with industry standards;
- 21 e. Whether Keenan owed a duty to Class Members to safeguard their PII
22 and PHI;
- 23 f. Whether Keenan was subject to (and breached) HIPAA, the FTC Act,
24 the California Confidentiality of Medical Information Act and/or the
25
26
27
28

1 CCPA;

2 g. Whether Keenan breached its duty to Class Members to safeguard their
3 PII and PHI;

4
5 h. Whether computer hackers obtained Class Members' PII and PHI in
6 the Data Breach;

7
8 i. Whether Keenan knew or should have known that its data security
9 systems and monitoring processes were deficient;

10 j. Whether Keenan's conduct was negligent;

11
12 k. Whether Keenan's acts breaching an implied contract they formed with
13 Plaintiff and the Class Members;

14
15 l. Whether Keenan was unjustly enriched to the detriment of Plaintiff and
16 the Class;

17 m. Whether Keenan failed to provide notice of the Data Breach in a timely
18 manner; and

19
20 n. Whether Plaintiff and Class Members are entitled to damages, civil
21 penalties, punitive damages, and/or injunctive relief.

22 75. **Typicality**: Plaintiff's claims are typical of those of other Class
23 Members because Plaintiff's PII and PHI, like that of every other Class Member,
24 was compromised in the Data Breach.
25

26 76. **Adequacy**: Plaintiff is an adequate representative for the Class
27 because his interests do not conflict with the interests of the Class that he seeks to
28

1 represent. Plaintiff has retained counsel competent and highly experienced in
2 complex class action litigation—including consumer fraud and automobile defect
3 class action cases—and counsel intends to prosecute this action vigorously. The
4 interests of the Class will be fairly and adequately protected by Plaintiff and his
5 experienced counsel.
6

7
8 77. **Superiority**: A class action is superior to all other available means of
9 fair and efficient adjudication of the claims of Plaintiff and members of the Class.
10 The injury suffered by each individual Class Member is relatively small in
11 comparison to the burden and expense of individual prosecution of the complex and
12 extensive litigation necessitated by Keenan's conduct. It would be virtually
13 impossible for members of the Class individually to redress effectively the wrongs
14 done to them by Keenan. Even if Class Members could afford such individual
15 litigation, the court system could not. Individualized litigation presents a potential
16 for inconsistent or contradictory judgments. Individualized litigation increases the
17 delay and expense to all parties, and to the court system, presented by the complex
18 legal and factual issues of the case. By contrast, the class action device presents far
19 fewer management difficulties, and provides the benefits of single adjudication, an
20 economy of scale, and comprehensive supervision by a single court. Upon
21 information and belief, members of the Class can be readily identified and notified
22 based upon, *inter alia*, the records (including databases, e-mails, dealership records
23 and files, etc.) Keenan maintains regarding their consumers.
24
25
26
27
28

78. Defendant has acted, and refuses to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

CLAIMS FOR RELIEF

COUNT I NEGLIGENCE

(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. Keenan owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII and PHI in its possession, custody, or control.

81. Keenan knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and PHI and the importance of maintaining secure systems. Keenan knew, or should have known, of the vast uptick in data breaches in recent years. Keenan had a duty to protect the PII and PHI of Plaintiff and Class Members.

82. Given the nature of Keenan's business, the sensitivity and value of the PII and PHI it maintains, and the resources at its disposal, Keenan should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Keenan had a duty to prevent.

1 83. Keenan breached these duties by failing to exercise reasonable care in
2 safeguarding and protecting Plaintiff's and Class Members' PII and PHI by failing
3 to design, adopt, implement, control, direct, oversee, manage, monitor, and audit
4 appropriate data security processes, controls, policies, procedures, protocols, and
5 software and hardware systems to safeguard and protect PII and PHI entrusted to
6 it—including Plaintiff's and Class Members' PII and PHI.
7

8
9 84. It was reasonably foreseeable to Keenan that its failure to exercise
10 reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII
11 and PHI by failing to design, adopt, implement, control, direct, oversee, manage,
12 monitor, and audit appropriate data security processes, controls, policies,
13 procedures, protocols, and software and hardware systems would result in the
14 unauthorized release, disclosure, and dissemination of Plaintiff's and Class
15 Members' PII and PHI to unauthorized individuals.
16
17

18 85. But for Keenan's negligent conduct or breach of the above-described
19 duties owed to Plaintiff and Class Members, their PII and PHI would not have been
20 compromised.
21

22 86. As a result of Keenan's above-described wrongful actions, inaction,
23 and want of ordinary care that directly and proximately caused the Data Breach,
24 Plaintiff and all other Class Members have suffered, and will continue to suffer,
25 economic damages and other injury and actual harm in the form of, *inter alia*: (i) a
26 substantially increased risk of identity theft—risks justifying expenditures for
27
28

1 protective and remedial services for which they are entitled to compensation; (ii)
2 improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their
3 PII; (iv) deprivation of the value of their PII and PHI, for which there is a well-
4 established national and international market; (v) lost time and money incurred to
5 mitigate and remediate the effects of the Data Breach, including the increased risks
6 of identity theft they face and will continue to face; and (vii) actual or attempted
7 fraud.
8

9
10 **COUNT II**
11 **NEGLIGENCE PER SE**
12 **(On Behalf of Plaintiff Rutledge and the Nationwide**
13 **Class or, alternatively, the California Class)**

14 87. Plaintiff realleges and incorporates by reference all preceding
15 paragraphs as if fully set forth herein.

16 88. Keenan's duties arise from Section 5 of the FTC Act ("FTCA"), 15
17 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce,"
18 including, as interpreted by the FTC, the unfair act or practice by a business, such as
19 Keenan, of failing to employ reasonable measures to protect and secure PII and
20 PHI.
21

22 89. Keenan violated Security Rules and Section 5 of the FTCA by failing
23 to use reasonable measures to protect Plaintiff's and all other Class Members' PII
24 and PHI and not complying with applicable industry standards. Keenan's conduct
25 was particularly unreasonable given the nature and amount of PII and PHI it obtains
26
27
28

1 and stores, and the foreseeable consequences of a data breach involving PII and PHI
2 including, specifically, the substantial damages that would result to Plaintiff and the
3 other Class Members.
4

5 90. Keenan's violations of Security Rules and Section 5 of the FTCA
6 constitutes negligence per se.
7

8 91. Plaintiff and Class Members are within the class of persons that
9 Security Rules and Section 5 of the FTCA were intended to protect.
10

11 92. The harm occurring as a result of the Data Breach is the type of harm
12 Security Rules and Section 5 of the FTCA were intended to guard against.
13

14 93. It was reasonably foreseeable to Keenan that its failure to exercise
15 reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII
16 and PHI by failing to design, adopt, implement, control, direct, oversee, manage,
17 monitor, and audit appropriate data security processes, controls, policies,
18 procedures, protocols, and software and hardware systems, would result in the
19 release, disclosure, and dissemination of Plaintiff's and Class Members' PII and
20 PHI to unauthorized individuals.
21

22 94. The injury and harm that Plaintiff and the other Class Members
23 suffered was the direct and proximate result of Keenan's violations of Security
24 Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and
25 will continue to suffer) economic damages and other injury and actual harm in the
26 form of, *inter alia*: (i) a substantially increased risk of identity theft—risks
27
28

1 justifying expenditures for protective and remedial services for which they are
 2 entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach
 3 of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII
 4 and PHI, for which there is a well-established national and international market; (v)
 5 lost time and money incurred to mitigate and remediate the effects of the Data
 6 Breach; and (vi) actual or attempted fraud.

9 **COUNT III**
 10 **BREACH OF FIDUCIARY DUTY**
 11 **(On Behalf of Plaintiff Rutledge and the Nationwide**
 12 **Class or, alternatively, the California Class)**

13 95. Plaintiff realleges and incorporates by reference all preceding
 14 paragraphs as if fully set forth herein.

15 96. Plaintiff and Class Members either directly or indirectly gave Keenan
 16 their PII and PHI in confidence, believing that Keenan would protect that
 17 information. Plaintiff and Class Members would not have provided Keenan with
 18 this information had they known it would not be adequately protected. Keenan's
 19 acceptance and storage of Plaintiff's and Class Members' PII and PHI created a
 20 fiduciary relationship between Keenan and Plaintiff and Class Members. In light of
 21 this relationship, Keenan must act primarily for the benefit of its consumers, which
 22 includes safeguarding and protecting Plaintiff's and Class Members' PII and PHI.

23 97. Keenan has a fiduciary duty to act for the benefit of Plaintiff and Class
 24 Members upon matters within the scope of their relationship. It breached that duty
 25

1 by failing to properly protect the integrity of the system containing Plaintiff's and
2 Class Members' PII and PHI, failing to safeguard the PII and PHI of Plaintiff and
3 Class Members it collected.
4

5 98. As a direct and proximate result of Keenan's breaches of its fiduciary
6 duties, Plaintiff and Class Members have suffered and will suffer injury, including,
7 but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the
8 compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses
9 associated with the prevention, detection, and recovery from unauthorized use of
10 their PII and PHI; (iv) lost opportunity costs associated with effort attempting to
11 mitigate the actual and future consequences of the Data Breach; (v) the continued
12 risk to their PII and PHI which remains in Keenan's possession; (vi) future costs in
13 terms of time, effort, and money that will be required to prevent, detect, and repair
14 the impact of the PII and PHI compromised as a result of the Data Breach; and (vii)
15 actual or attempted fraud.
16
17
18
19

20 **COUNT IV**
21 **UNJUST ENRICHMENT**
22 **(On Behalf of Plaintiff Rutledge and the Nationwide**
23 **Class or, alternatively, the California Class)**

23 99. Plaintiff realleges and incorporates by reference all preceding
24 paragraphs as if fully set forth herein. This claim is pleaded in the alternative to the
25 implied contract claim pursuant to Fed. R. Civ. P. 8(d).
26

27 100. Plaintiff and Class Members conferred a monetary benefit upon
28

1 Keenan in the form of monies paid for production services or other services.

2 101. Keenan accepted or had knowledge of the benefits conferred upon it by
3
4 Plaintiff and Class Members. Keenan also benefitted from the receipt of Plaintiff's
5 and Class Members' PII and PHI.

6 102. As a result of Keenan's conduct, Plaintiff and Class Members suffered
7
8 actual damages in an amount equal to the difference in value between their
9 payments made with reasonable data privacy and security practices and procedures
10 that Plaintiff and Class Members paid for, and those payments without reasonable
11 data privacy and security practices and procedures that they received.

12
13 103. Keenan should not be permitted to retain the money belonging to
14
15 Plaintiff and Class Members because Keenan failed to adequately implement the
16 data privacy and security procedures for itself that Plaintiff and Class Members paid
17 for and that were otherwise mandated by federal, state, and local laws. and industry
18 standards.

19
20 104. Keenan should be compelled to provide for the benefit of Plaintiff and
21
22 Class Members all unlawful proceeds received by it as a result of the conduct and
23 Data Breach alleged herein.

24 **COUNT V**
25 **BREACH OF IMPLIED CONTRACT**
26 **(On Behalf of Plaintiff Rutledge and the Nationwide**
 Class or, alternatively, the California Class)

27 105. Plaintiff realleges and incorporates by reference all allegations of the
28

1 preceding factual allegations as though fully set forth herein.

2 106. Defendant required Plaintiff and Class Members to provide, or
3 authorize the transfer of, their PII and PHI in order for Keenan to provide services.
4 In exchange, Keenan entered into implied contracts with Plaintiff and Class
5 Members in which Keenan agreed to comply with its statutory and common law
6 duties to protect Plaintiff's and Class Members' PII and PHI and to timely notify
7 them in the event of a data breach.
8

9
10 107. Plaintiff and Class Members would not have provided their PII and
11 PHI to Keenan had they known that Keenan would not safeguard their PII and PHI,
12 as promised, or provide timely notice of a data breach.
13

14 108. Plaintiff and Class Members fully performed their obligations under
15 their implied contracts with Keenan.
16

17 109. Defendant breached the implied contracts by failing to safeguard
18 Plaintiff's and Class Members' PII and PHI and by failing to provide them with
19 timely and accurate notice of the Data Breach.
20

21 110. The losses and damages Plaintiff and Class Members sustained (as
22 described above) were the direct and proximate result of Keenan's breach of its
23 implied contracts with Plaintiff and Class Members.
24
25
26
27
28

COUNT VI
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018
Cal. Civ. Code §§ 1798.100 *et seq.* (“CCPA”)
(On Behalf of Plaintiff Rutledge and the Nationwide
Class or, alternatively, the California Class)

111. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

112. As more personal information about consumers is collected by businesses, consumers’ ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

113. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

114. Keenan is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

115. Section 1798.150(a)(1) of the CCPA provides: “Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security

1 procedures and practices appropriate to the nature of the information to protect the
2 personal information may institute a civil action for” statutory or actual damages,
3 injunctive or declaratory relief, and any other relief the court deems proper.
4

5 116. Plaintiff is a “consumer” as defined by Civ. Code § 1798.140(g)
6 because he is natural person residing in the state of California.
7

8 117. Keenan is a “business” as defined by Civ. Code § 1798.140(c).

9 118. The CCPA provides that “personal information” includes “[a]n
10 individual’s first name or first initial and the individual’s last name in combination
11 with any one or more of the following data elements, when either the name or the
12 data elements are not encrypted or redacted . . . (iii) Account number or credit or
13 debit card number, in combination with any required security code, access code, or
14 password that would permit access to an individual’s financial account.” *See* Civ.
15 Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).
16
17

18 119. Plaintiff’s Private Information compromised in the Data Breach
19 constitutes “personal information” within the meaning of the CCPA.
20

21 120. Through the Data Breach, Plaintiff’s private information was accessed
22 without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or
23 nonredacted format.
24

25 121. The Data Breach occurred as a result of Keenan’s failure to implement
26 and maintain reasonable security procedures and practices appropriate to the nature
27 of the information.
28

1 122. Simultaneously herewith, Plaintiff is providing notice to Defendants
2 pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of
3 the CCPA. Plaintiff alleges Keenan has violated or is violating. Although a cure is
4 not possible under the circumstances, if (as expected) Keenan is unable to cure or
5 does not cure the violation within 30 days, Plaintiff will amend this Complaint to
6 pursue actual or statutory damages as permitted by Cal. Civ. Code §
7 1798.150(a)(1)(A).
8

9
10 123. As a result of Keenan's failure to implement and maintain reasonable
11 security procedures and practices that resulted in the Data Breach, Plaintiff seeks
12 statutory damages of up to \$750 per class member (and no less than \$100 per class
13 member), actual damages to the extent they exceed statutory damages, injunctive
14 and declaratory relief, and any other relief as deemed appropriate by the Court.
15
16

17 **COUNT VII**
18 **VIOLATION OF THE CALIFORNIA CONSUMER LEGAL**
19 **REMEDIES ACT**

20 **Cal. Civ. Code §§ 1750 et seq. ("CLRA")**
21 **(On Behalf of Plaintiff Rutledge and the Nationwide**
22 **Class or, alternatively, the California Class)**

23 124. Plaintiff realleges and incorporates by reference each and every
24 allegation contained elsewhere in this Complaint as if fully set forth herein.

25 125. This cause of action is brought pursuant to the California Consumers
26 Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This
27 cause of action does not seek monetary damages at this time but is limited solely to
28

1 injunctive relief. Plaintiff will later amend this Complaint to seek damages in
2 accordance with the CLRA after providing Defendants with notice required by
3 California Civil Code § 1782.
4

5 126. Plaintiff and Class Members are “consumers,” as the term is defined by
6 California Civil Code § 1761(d).
7

8 127. Plaintiff, Class Members and Defendants have engaged in
9 “transactions,” as that term is defined by California Civil Code § 1761(e).
10

11 128. The conduct alleged in this Complaint constitutes unfair methods of
12 competition and unfair and deceptive acts and practices for the purpose of the
13 CLRA, and the conduct undertaken by Defendants was likely to deceive consumers.
14

15 129. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a
16 transaction from “[r]epresenting that goods or services have sponsorship, approval,
17 characteristics, ingredients, uses, benefits, or quantities which they do not have.”
18

19 130. Defendants violated this provision by representing that Defendants
20 took appropriate measures to protect Plaintiff’s and the Class Members’ PII and
21 PHI. Additionally, Defendants improperly handled, stored, or protected either
22 unencrypted or partially encrypted data.
23

24 131. As a result, Plaintiff and the Class Members were induced to provide
25 their PII and PHI to Defendants.
26

27 132. As a result of engaging in such conduct, Defendants have violated
28 Civil Code § 1770.

1 133. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order
2 of this Court that includes, but is not limited to, an order enjoining Defendants from
3 continuing to engage in unlawful, unfair, or fraudulent business practices or any
4 other act prohibited by law.
5

6 134. Plaintiff and the Class Members suffered injuries caused by
7 Defendants' misrepresentations, because they provided their PII and PHI believing
8 that Defendants would adequately protect this information.
9

10 135. Plaintiff and Class Members may be irreparably harmed and/or denied
11 an effective and complete remedy if such an order is not granted.
12

13 136. The unfair and deceptive acts and practices of Defendants, as described
14 above, present a serious threat to Plaintiff and members of the Class.
15

16 **COUNT VIII**
17 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW**
18 **Cal. Bus. and Prof. Code §§ 17200, *et seq.* ("UCL")**
19 **(On Behalf of Plaintiff Rutledge and the Nationwide**
20 **Class or, alternatively, the California Class)**

21 137. Plaintiff re-alleges and incorporates by reference all preceding factual
22 allegations as though fully set forth herein.
23

24 138. Plaintiffs brings this claim on behalf of themselves and the Class.
25

26 139. The California Unfair Competition Law, Cal. Bus. & Prof. Code
27 §17200, *et seq.* ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair"
28 business act or practice and any false or misleading advertising, as defined by the
UCL and relevant case law.

1 140. By reason of Defendants' above-described wrongful actions, inaction,
2 and omission, the resulting Data Breach, and the unauthorized disclosure of
3 Plaintiff's and Class members' PII and PHI, Defendants engaged in unlawful, unfair
4 and fraudulent practices within the meaning of the UCL.
5

6 141. Defendants' business practices as alleged herein are unfair because
7 they offend established public policy and are immoral, unethical, oppressive,
8 unscrupulous and substantially injurious to consumers, in that the private and
9 confidential PII and PHI of consumers has been compromised for all to see, use, or
10 otherwise exploit.
11

12 142. Defendants' practices were unlawful and in violation of the CCPA and
13 CLRA and Defendants' own privacy policy because Defendants Yahoo failed to
14 take reasonable measures to protect Plaintiff's and Class members' PII and PHI.
15

16 143. Defendants' business practices as alleged herein are fraudulent because
17 they are likely to deceive consumers into believing that the PII and PHI they
18 provide to Defendants will remain private and secure, when in fact it was not
19 private and secure.
20

21 144. Plaintiff and Class Members suffered (and continue to suffer) injury in
22 fact and lost money or property as a direct and proximate result of Defendants'
23 above-described wrongful actions, inaction, and omissions including, *inter alia*, the
24 unauthorized release and disclosure of their PII and PHI.
25

26 145. Defendants' above-described wrongful actions, inaction, and
27
28

1 omissions, the resulting Data Breach, and the unauthorized release and disclosure of
2 Plaintiff's and Class Members' PII and PHI also constitute "unfair" business acts
3 and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq.*, in that
4 Defendants' conduct was substantially injurious to Plaintiff and Class Members,
5 offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the
6 gravity of Defendants' conduct outweighs any alleged benefits attributable to such
7 conduct.
8

9
10 146. But for Defendant's misrepresentations and omissions, Plaintiff and
11 Class Members would not have provided their PII and PHI to Defendants, or would
12 have insisted that their PII and PHI be more securely protected.
13

14 147. As a direct and proximate result of Defendants' above-described
15 wrongful actions, inaction, and omissions, the resulting Data Breach, and the
16 unauthorized release and disclosure of Plaintiff and Class Members' PII and PHI,
17 they have been injured as follows: (1) the loss of the opportunity to control how
18 their PII and PHI is used; (2) the diminution in the value and/or use of their PII and
19 PHI entrusted to Defendants; (3) the increased, imminent risk of fraud and identity
20 theft; (4) the compromise, publication, and/or theft of their PII and PHI; and (5)
21 costs associated with monitoring their PII and PHI, amongst other things.
22
23

24 148. Plaintiff takes upon himself enforcement of the laws violated by
25 Defendants in connection with the reckless and negligent disclosure of PII and PHI.
26 There is a financial burden incurred in pursuing this action and it would be against
27
28

1 the interests of justice to penalize Plaintiff by forcing him to pay attorneys' fees and
2 costs from the recovery in this action. Therefore, an award of attorneys' fees and
3 costs is appropriate under California Code of Civil Procedure § 1021.5.
4

5 **COUNT IX**
6 **VIOLATIONS OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL**
7 **INFORMATION ACT, Cal. Civ. Code 56 *et seq.* ("CMIA")**
8 **(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the**
9 **California Class)**

10 71. Plaintiff realleges and incorporates by reference every paragraph set
11 forth in this Complaint as if fully set forth herein.

12 72. Plaintiff brings this count on behalf of himself and the California
13 Class.

14 73. Keenan is a "Contractor" as defined by Cal. Civ. Code § 56.05(d)
15 and/or a "Provider of Health Care" as expressed in Cal. Civ. Code § 56.06, and is
16 therefore subject to the requirements of the CMIA.
17

18 74. Plaintiff and members of the California Class are "Patients" as defined
19 by Cal. Civ. Code § 56.05(k).
20

21 75. Plaintiff and California Class Members' Private Information that was
22 subject to the Data Breach included "Medical Information" as defined by Cal. Civ.
23 Code §56.05(j).
24

25 76. In violation of Cal. Civ. Code § 56.10(a), Keenan disclosed medical
26 information (including Plaintiffs' Private Information) without first obtaining an
27 authorization. The unauthorized disclosure of Plaintiff's and California Class
28

1 Members' Private Information to unauthorized individuals in the Data Breach
2 resulted from the affirmative actions of Keenan, who placed two file directories on
3 a web server that was exposed to the public internet. Disclosing Plaintiff's and
4 California Class Members' Private Information on the internet was an affirmative
5 communicative act by Keenan and a violation of Cal. Civ. Code § 56.10(a).
6 Plaintiff's and California Class Members' Private Information was viewed and
7 accessed by unauthorized individuals as a direct and proximate result of Keenan's
8 violation of Cal. Civ. Code § 56.10(a).
9

10
11
12 77. In violation of Cal. Civ. Code § 56.101(a), Keenan created,
13 maintained, preserved, stored, abandoned, destroyed, or disposed of medical
14 information (including Plaintiff's and California Class Members' Private
15 Information) in a manner that failed to preserve and breached the confidentiality of
16 the information contained therein. This violation resulted from the affirmative
17 actions of Keenan or its agents who exposed two file servers containing Private
18 Information on the public internet. This disclosure was an affirmative
19 communicative act by Keenan and a violation of Cal. Civ. Code § 56.101(a).
20 Plaintiff's and California Class Members' Private Information was viewed by
21 unauthorized individuals as a direct and proximate result of Keenan's violation of
22 Cal. Civ. Code § 56.101(a).
23

24
25
26 78. Keenan further violated § 56.101(a) because Keenan negligently
27 created, maintained, preserved, stored, abandoned, destroyed, or disposed of
28

1 medical information (including Plaintiff's and California Class Members' Private
2 Information). This violation resulted from the affirmative actions of Keenan or its
3 agents who exposed two file servers containing Private Information on the public
4 internet. This disclosure was an affirmative communicative act by Keenan and a
5 violation of Cal. Civ. Code § 56.101(a). Plaintiff's and California Class Members'
6 Private Information was viewed by unauthorized individuals as a direct and
7 proximate result of Keenan's violation of Cal. Civ. Code § 56.101(a).
8
9

10 79. Plaintiff's and California Class Members' Private Information that was
11 the subject of the Data Breach included "electronic medical records" or "electronic
12 health records" as referenced by Cal. Civ. Code § 56.101(c) and defined by 42
13 U.S.C. § 17921(5).
14
15

16 80. In violation of Cal. Civ. Code § 56.101(b)(1)(A), Keenan's electronic
17 health record system or electronic medical record system failed to protect and
18 preserve the integrity of electronic medical information (including Plaintiff's and
19 California Class Members' Private Information). This violation resulted from the
20 affirmative actions of Keenan or its agents who exposed two file servers containing
21 Private Information on the public internet. This disclosure was an affirmative
22 communicative act by Keenan and a violation of Cal. Civ. Code § 56.101(b)(1)(A).
23 Plaintiff's and California Class Members' Private Information was viewed by
24 unauthorized individuals as a direct and proximate result of Keenan's violation of
25 Cal. Civ. Code § 56.101(b)(1)(A).
26
27
28

1 81. In violation of Cal. Civ. Code § 56.101(b)(91)(B), Keenan's electronic
2 health record system or electronic medical record system failed to automatically
3 record and preserve any change or deletion of any electronically stored medical
4 information (including Plaintiff Rutledge's and California Class Members' Private
5 Information).
6

7 82. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Keenan's electronic
8 health record system or electronic medical record system failed to record the
9 identity of persons who accessed and changed medical information, failed to record
10 the date and time medical information was accessed, and failed to record changes
11 that were made to medical information.
12

13 83. In violation of Cal. Civ. Code § 56.26(a) Keenan, as an entity engaged
14 in the business of furnishing administrative services to health care providers or their
15 affiliates, knowingly used, disclosed, or permitted its employees or agents to use or
16 disclose medical information possessed in connection with performing
17 administrative functions for a program, in a manner not reasonably necessary in
18 connection with the administration or maintenance of the program, or in a manner
19 not required by law, or without authorization. This violation resulted from the
20 affirmative actions of Keenan or its agents who exposed two file servers containing
21 Private Information on the public internet. This disclosure was an affirmative
22 communicative act by Keenan and a violation of Cal. Civ. Code § 56.26(a).
23 Plaintiff's and California Class Members' Private Information was viewed by
24
25
26
27
28

1 unauthorized individuals as a direct and proximate result of Keenan's violation of §
2 56.26(a).

3
4 84. In violation of Cal. Civ. Code § 56.36(b), Keenan negligently released
5 confidential information or records concerning Plaintiff Rutledge and California
6 Class Members. This negligent release of Plaintiff Rutledge's and California Class
7 Members' Private Information to unauthorized individuals in the Data Breach
8 resulted from the affirmative actions of Keenan or its agents who exposed two file
9 servers containing Private Information on the public internet. This disclosure was an
10 affirmative act by Keenan and a violation of Cal. Civ. Code § 56.36(b). Plaintiff
11 Rutledge's and California Class Members' Private Information was viewed by
12 unauthorized individuals as a direct and proximate result of Keenan's violation of
13 Cal. Civ. Code § 36.36(b).

14
15
16
17 85. In violation of Cal. Civ. Code § 56.10(d), Keenan intentionally shared,
18 sold, used for marketing, or otherwise used Plaintiff's and California Class
19 Members' Private Information for a purpose not necessary to provide health
20 services to Plaintiff or California Class Members.

21
22 86. In violation of Cal. Civ. Code § 56.10(e), Keenan further disclosed
23 Plaintiff's and California Class Members' Private Information to persons or entities
24 not engaged in providing direct health care services to Plaintiff's or California Class
25 Members or their providers of health care of health care service plans or insurers or
26 self-insured employers.
27
28

1 87. All of Keenan's acts described herein were done knowingly and
2 willfully by Keenan.

3
4 88. Plaintiff and California Class Members were injured and have suffered
5 damages, as described herein, from Keenan's illegal disclosure and negligent
6 release of their Private Information in violation of Cal. Civ. Code §§ 56.10, 56.101,
7 56.26 and 56.36 and therefore seek relief under Civ. Code §§ 56.35 and 56.36,
8 including actual damages, nominal statutory damages of \$1,000, punitive damages
9 of \$3,000, injunctive relief, and attorneys' fees, expenses and costs.
10

11
12 89. As a direct and proximate result of Keenan's violations of the CMIA,
13 Plaintiff and California Class Members have faced and will face an increased risk of
14 future harm.

15
16 90. As a direct and proximate result of Keenan's violations of the CMIA,
17 Plaintiff and California Class Members have suffered injury and are entitled to
18 damages in an amount to be proven at trial.

19
20 91. Plaintiff and California Class Members suffered a privacy injury by
21 having their sensitive medical information disclosed, irrespective of whether or not
22 they subsequently suffered identity fraud, or incurred any mitigation damages.
23 Medical information has been recognized as private sensitive information in
24 common law and federal and state statutory schemes and the disclosure of such
25 information resulted in cognizable injury to Plaintiff and California Class Members.
26
27
28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, pray for judgment as follows:

- a. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;
- b. For equitable relief enjoining Keenan from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI;
- c. For equitable relief compelling Keenan to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;
- d. For an order requiring Keenan to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;
- e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- f. For an award of punitive damages, as allowable by law;
- g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- h. Pre and post-judgment interest on any amounts awarded; and
- i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 2, 2024

Respectfully submitted by:

By: /s/ Jonathan Shub

Jonathan Shub (No. 237708)

Benjamin F. Johns*

Samantha E. Holbrook*

SHUB & JOHNS LLC

Four Tower Bridge

200 Barr Harbor Drive, Suite 400

Conshohocken, PA 19428

(610) 477-8380

jshub@shublawayers.com

bjohns@shublawayers.com

sholbrook@shublawayers.com

*Attorneys for Plaintiff and the
Proposed Class*

**Pro Hac Vice Forthcoming*